AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Western District of Wisconsin

In the Matter of the Search of Information associated with Apple ID sire.gq@icloud.com that is stored at premises controlled by Apple	)	Case No. 20-mj-80 **SEALED**

APPLICATION FOR A SEARCH WARRANT

I, William Fulton, a federal law enforcement officer, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:

See Attachment A.

located in the Northern District of California, there is now concealed:

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 844(i)	Causing damage to property by fire or explosives

The application is based on these facts: See attached Affidavit.

Applicant's signature

William Fulton, ATF Special Agent

Printed name and title

Sworn to before me and signed in my presence.

Date: 7/10/20

Judge's signature

Madison, Wisconsin

Magistrate Judge Stephen L. Crocker or
Magistrate Judge Peter A. Oppeneer

AFFIDAVIT

STATE OF WISCONSIN)
) ss.
DANE COUNTY)

I, William Fulton, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. This affidavit is being made in support of an application for issuance of a search warrant for the contents of an iCloud account with Apple ID of sire.gq@icloud.com ("the Target Account").

2. The Target Account is associated with a black iPhone ("Target Telephone") which I believe belongs to Marquon CLARK. The Target Account is further described in Attachment A.

3. I am a Special Agent of the United States Justice Department, Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), currently assigned to the Madison Field Office. I have been so employed since July of 2009. I am a graduate of the Federal Law Enforcement Training Center Criminal Investigator Training Program, the Department of Justice, Bureau of Alcohol Tobacco Firearms and Explosives Special Agent Basic Training, and have received extensive training to qualify as an expert in fire origin and cause investigations. Prior to my employment with the ATF, I was employed as a local fire marshal/fire investigator/fire fighter in the state of Virginia from June 1997 to December 2008.

4. It is my experience that many individuals involved in various crimes will utilize telephones to promote their criminal activity and that records related to the use of telephones often provide information regarding the Internet and all Internet instrumentalities, such as e-mail, social media, and other Internet-based programs, to conduct, promote, and facilitate their illegal activities. I have been involved with many criminal investigations, including arson cases, in which individuals utilized cellular telephones to facilitate their crimes.

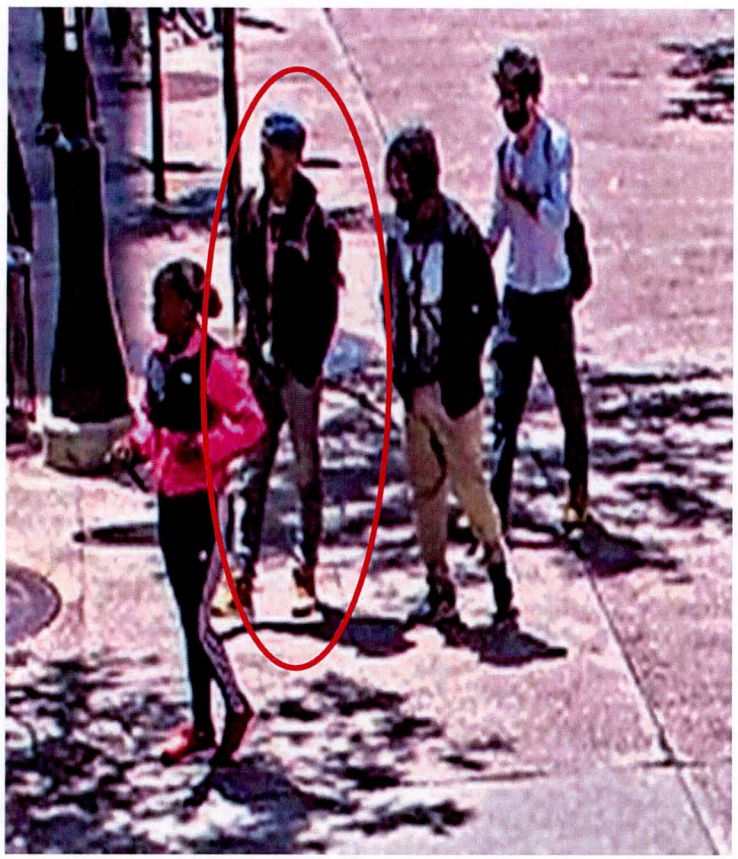
5. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

6. The Target Account is maintained by Apple, Inc. (hereinafter "Apple"), headquartered at 1 Infinite Loop, Cupertino, California. Based on the facts set forth in this affidavit, there is probable cause to believe that the user of the Target Account has violated the following: 18 U.S.C. § 844(i), causing damage by fire or explosive.

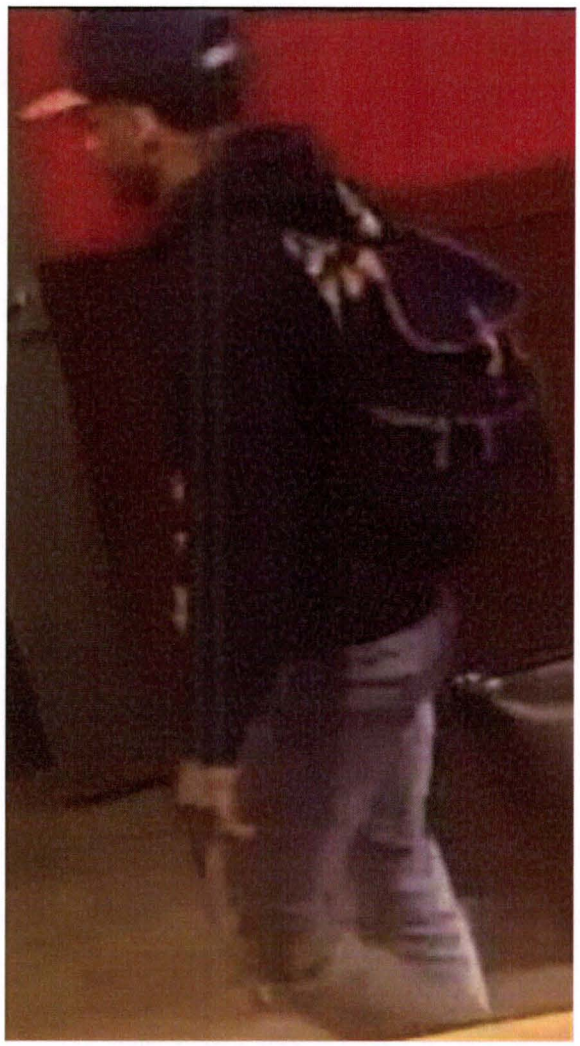
PROBABLE CAUSE

7. On June 23, 2020, surveillance cameras show Marquon CLARK walking around different locations in downtown Madison. The following photographs from June 23 were shown to Madison Police Department Sergeant Shannon Blackamore. Sergeant Blackamore has arrested CLARK on one previous occasion and had about five other professional contacts with him. In each of the three photographs below, Sergeant Blackmore identified CLARK as the individual circled in red, who is wearing a dark

colored straight brim hat with tan brim, a black hoodie sweatshirt, faded jeans, brown shoes, and carrying a dark colored back pack with tan/brown arm straps. In addition, I have identified Taliya BROWN as the woman walking with CLARK and wearing a black and pink North Face jacket.



7. In addition, I recognize CLARK from the following picture taken on June 23 from a business in downtown Madison. In the picture, I noticed that the rear of CLARK's backpack has contrasting piping.

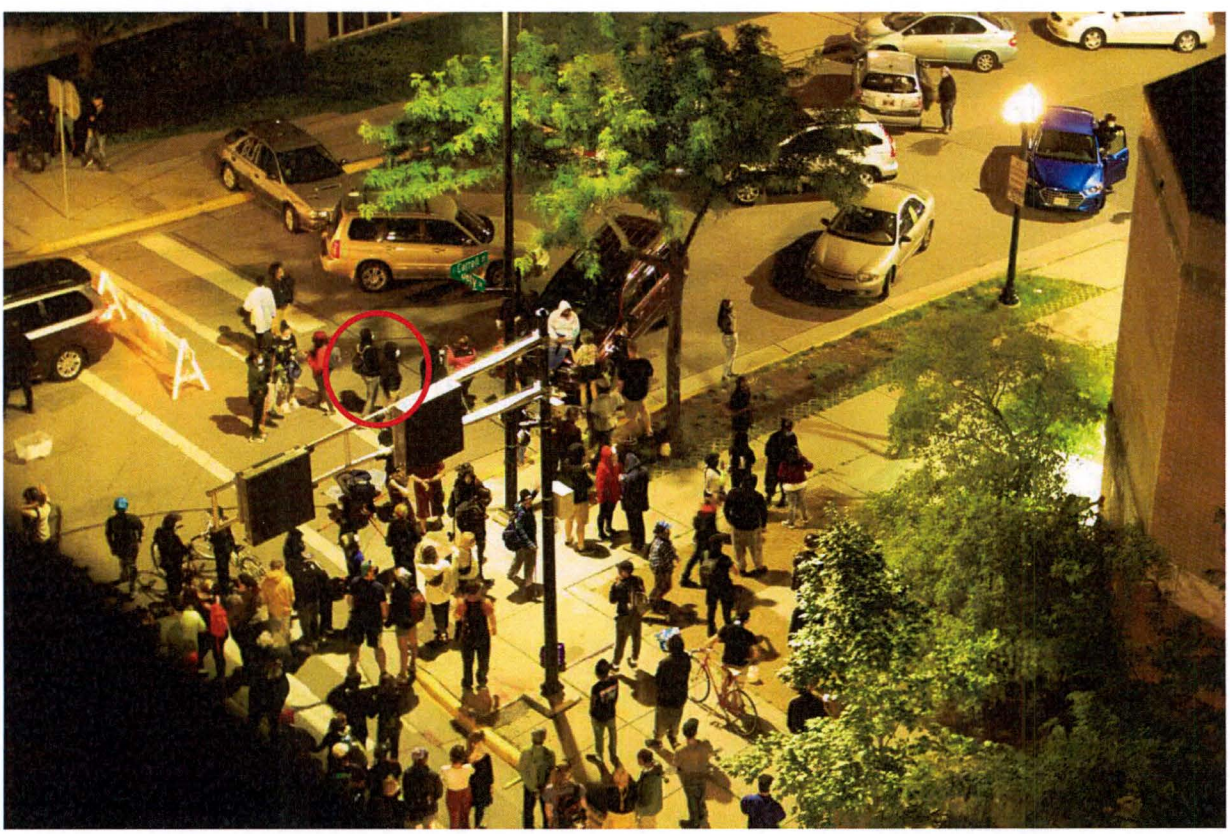


8. In the early evening on June 23, 2020, protestors in downtown Madison surrounded a commercial tow truck. The tow truck was abandoned in front of the Dane County Courthouse, at South Hamilton Street and North Henry Street, which is located one block from the City-County Building (CCB) located at 210 Martin Luther Blvd. Protesters caused the driver to evacuate and abandon his vehicle. A YouTube video shows CLARK, standing on top of the tow truck, recording a video.[1] During the

[1] https://www.youtube.com/watch?v=RawI6Rq44uU

video, CLARK makes the following statements - "We got a mother fucking tow truck," "Fuck12," "We going to get that mother fucker, I promise you," "it's a revolution, come downtown tonight it's a about to go down, nigga." A still image of CLARK from the video is below.

9. Later that night, at approximately 10:25 p.m., a group of approximately 10 to 12 cars were parked and blocking traffic in the roadway on the 200 block of S. Carroll Street in Madison. The vehicles appeared to be unoccupied and blocked the roadway between the CCB and the Dane County Public Safety Building (PSB).[2] In the photograph below, CLARK can been seen wearing a dark colored straight brim hat with tan brim, a black hoodie sweatshirt, a white face covering, faded jeans, and brown shoes. He is wearing the same dark colored backpack with tan/brown arm straps and contrasting piping that he was seen wearing earlier in the day.

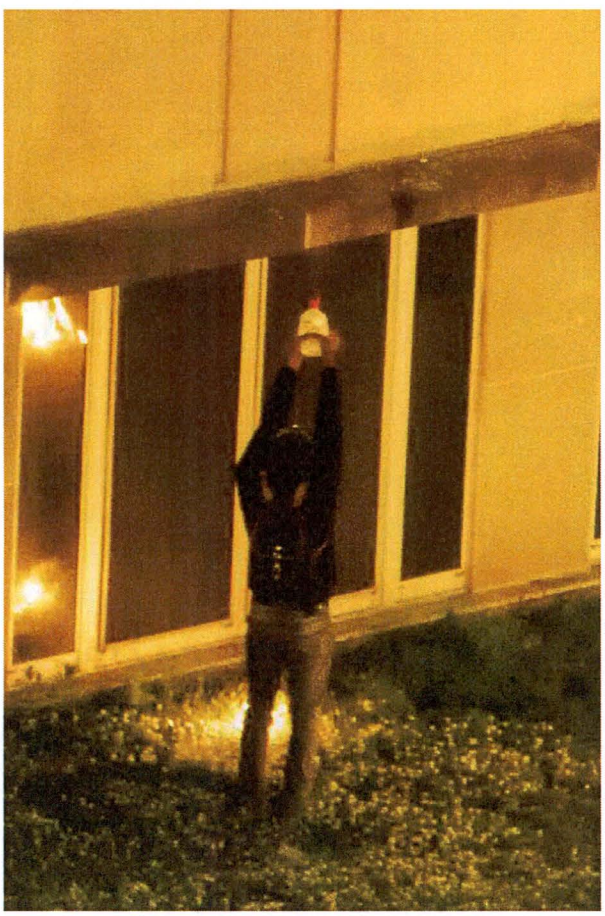


[2] I am aware that the CCB houses the Madison Police Department, Dane County Dispatch (911 call center), and other city and county government offices.

10. On June 24, 2020, at approximately 12:32 a.m., a citizen approached the closed CCB garage door and communicated with police officers on the inside. The citizen informed officers that the group of people were threatening to start fires on the Carroll Street side of the CCB.

11. On June 24, 2020, at approximately 12:41 a.m., Dane County Dispatch employees heard glass breaking near their workspace and smoke was observed in the building. The CCB's fire alarms were then activated and employees began to evacuate the building.

12. Photographs from the exterior of the CCB building taken at same time show CLARK throwing rocks through the windows of the CCB. After the windows were broken, CLARK threw a lit roll of paper towels into the CCB starting a fire, as depicted in the photographs below. In the photographs, CLARK is wearing the same dark colored backpack with tan/brown arm straps and contrasting piping that he was seen wearing earlier in the day.

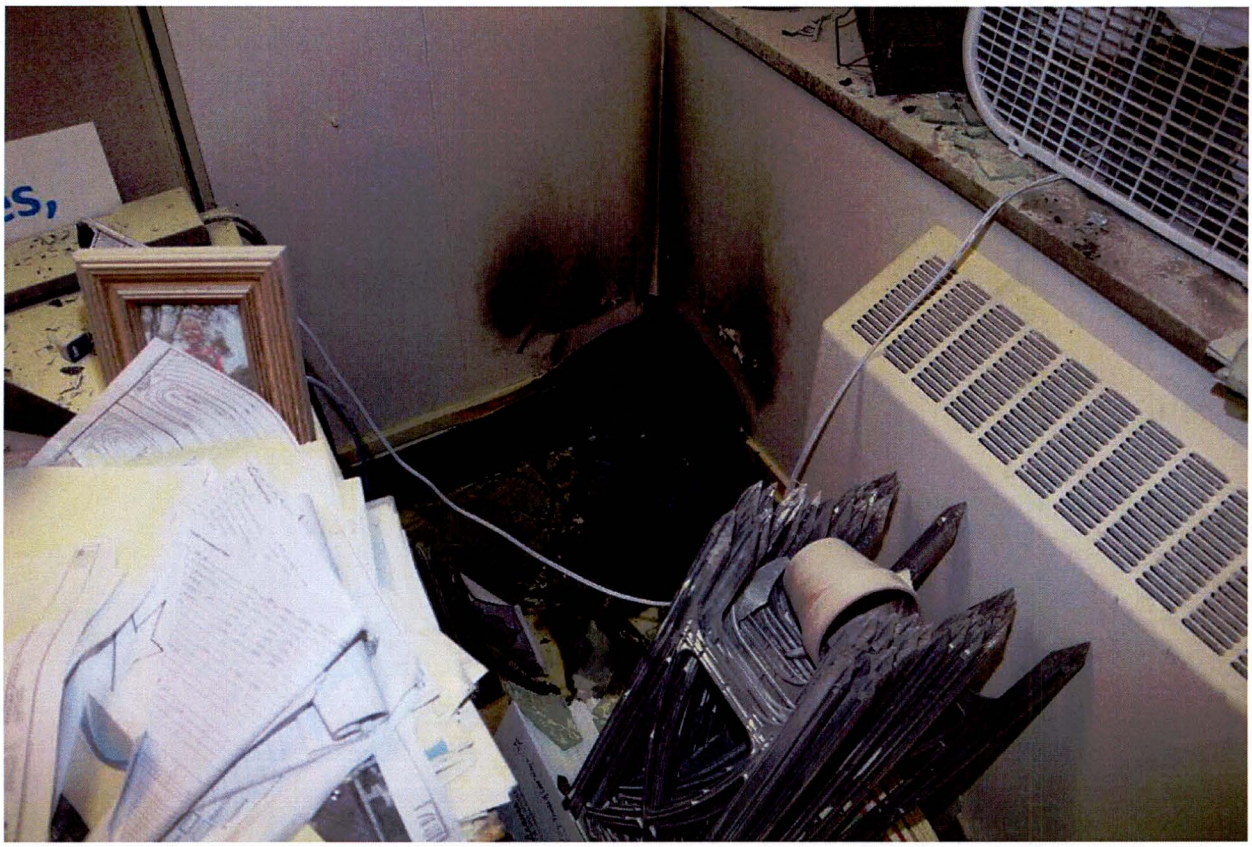


13. The following three photographs from the exterior of the CCB show a person resembling BROWN (wearing a pink and black North Face jacket) at the scene with CLARK.

14. At the time CLARK set the CCB on fire, it was occupied by over 250 people. Officers responding to the CCB noticed a clear plastic bottle with a burned wick in the neck of the bottle, outside of the building.

Inside the CCB, at the scene of the fire, investigators located a clear plastic bottle with a burned neck inside the building as well.

The quick actions of the deputies from the Dane County Sheriff's Office prevented the fire from extending beyond the cubical and its contents.



The Madison Fire Department responded to the extinguished fire to ventilate the building. The Madison Fire Investigation Team responded to the scene to conduct the origin and cause investigation. The Madison Fire Investigation Team determined the fire was intentionally set, and classified the fire as Incendiary.

15. The CCB is the property of the City of Madison and Dane County. Both the City of Madison and Dane County conduct business in interstate commerce, for instance by purchasing vehicles and other equipment and supplies in interstate

commerce. The activities of the City of Madison and Dane County in enacting and enforcing laws also affect interstate commerce

16. During the course of my investigation, I found a Facebook account that appears to belong to CLARK - https://www.facebook.com/sire.gq. I know that "Sire GQ" is a nickname used by CLARK. As I reviewed the account, I saw numerous Facebook Live videos taken by CLARK on June 21, 2020, as he helped lead protests in downtown Madison. In one of the videos from that day, he can be seen and heard leading the following chant – "If we don't get it, burn it down."

17. I am aware that CLARK is currently on supervision through the Wisconsin Department of Corrections. CLARK's registered telephone with the Wisconsin Department of Corrections is (608) 716-9112. On June 16, 2020, Stuart Liverseed, a probation agent with the Wisconsin Department of Corrections, called (608) 716-9112 and spoke with CLARK.

18. On June 17, 2020, an individual called the Madison Police Department and identified himself as "Sire." "Sire" stated that a group was organizing a community car wash along West Washington Avenue and Park St. in Madison. When asked for a cellular telephone number, "Sire" provided (608) 716-9112.

19. On June 30, 2020, officers interviewed CLARK's mother and his grandmother. When asked for CLARK's cellular telephone number, both his grandmother and his mother provided (608) 716-9112.

20. On June 30, 2020, officers stopped a 2007 white Chevrolet Malibu with Wisconsin license plate number AAR7825 ("the Malibu") on Verona Road in Madison. CLARK was driving the Malibu and BROWN was in the front passenger seat. The Malibu is registered to BROWN. CLARK was arrested for a parole warrant and he did not have a cellular telephone in his possession. BROWN was detained and released and she did have cellular telephone in her possession. The Malibu was towed away from the scene because BROWN did not have a valid driver's license.

21. On July 1, 2020, Magistrate Judge Stephen Crocker, Western District of Wisconsin, signed a search warrant for the Malibu. During the search, officers found the Target Telephone on the front passenger's seat on top of a pale blue shirt.

22. On June 17, Kimberley Bizub, a Digital Forensics Examiner with the Wisconsin Department of Justice (DCI), connected the Target Telephone to a GrayKey machine but was unable to access the phone's contents due to password restrictions. However, Bizub performed a partial extraction on the Target Telephone. As a result of the partial extraction, Bizub learned that the Target Telephone has an associated telephone number of (608) 716-9112 and an Apple ID of sire.gq@icloud.com.

BACKGROUND REGARDING APPLE ID AND iCLOUD

23. Through my training and experience, as well as information provided to me by other experienced law enforcement officers, I know that Apple is a United States company that produces the iPhone, iPad, iPod Touch and Apple Watch, all of which

use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

24. Through my training and experience, as well as information provided to me by other experienced law enforcement officers, I know that Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications ("apps"). As described in further detail below, the services include email, instant messaging, and file storage.

25. Through my training and experience, as well as information provided to me by other experienced law enforcement officers, I know that Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

26. Through my training and experience, as well as information provided to me by other experienced law enforcement officers, I know that iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages ("iMessages") containing texts, photos, videos, locations, and contacts, while FaceTime enables those users to conduct video calls.

27. Through my training and experience, as well as information provided to me by other experienced law enforcement officers, I know that iCloud-connected services allow users to create, store, access, share, and synchronize data on Apple

devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on icloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs enables iCloud to be used to synchronize webpages opened in the Safari web browsers on all of the user's Apple devices. iWorks Apps, a suite of productivity apps (Pages, Numbers, and Keynote), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

28. Through my training and experience, as well as information provided to me by other experienced law enforcement officers, I know that Apple services are accessed through the use of an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

29. Through my training and experience, as well as information provided to me by other experienced law enforcement officers, I know that an Apple ID takes the form of the full email address submitted by the user to create the account; it can later be

changed. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a "verification email" sent by Apple to that "primary" email address. Additional email addresses ("alternate," "rescue," and "notification" email addresses) can also be associated with an Apple ID by the user.

30. Through my training and experience, as well as information provided to me by other experienced law enforcement officers, I know that Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user's full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the "My Apple ID" and "iForgot" pages on Apple's website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address ("IP address") used to register and access the account, and other log files that reflect usage of the account.

31. Through my training and experience, as well as information provided to me by other experienced law enforcement officers, I know that additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

32. Through my training and experience, as well as information provided to me by other experienced law enforcement officers, I know that Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs in to FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is

used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

33. Through my training and experience, as well as information provided to me by other experienced law enforcement officers, I know that Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWorks and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud.

34. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

35. Through my training and experience, as well as information provided to me by other experienced law enforcement officers, I know that other information connected to an Apple ID may provide direct evidence of the offenses under investigation. Based on my training and experience, I know that instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the drug trafficking offense under investigation.

36. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

37. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App

Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crime under investigation.

38. In addition, iCloud backups of a computer, its storage devices, peripherals, and Internet connection interface may be instrumentalities of the crimes, within the meaning of 18 U.S.C. §§ 2251 through 2256, and is subject to seizure as such if they were used to facilitate the drug trafficking crime under investigation.

39. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning the subscriber of the Target Address and their use of Apple's services. Because it appears that NORRIS was actively involved in drug trafficking at the time the Target Telephone was seized, I believe there is probable cause to believe that the Target Account will contain evidence of the drug trafficking crime under investigation including information that can be used to identify the account's user or users.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

35. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Apple to disclose to the government copies of the records and other information (including the content of communications and stored data)

particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

36. I request that the Court order Apple not to notify any person (including the subscribers or customers of the account listed in Attachment A) of the existence of the requested warrant before January 8, 2021 until further order of the Court. Apple Inc. is a provider of an electronic communication service, as defined in 18 U.S.C. § 2510(15), and/or a remote computer service, as defined in 18 U.S.C. § 2711(2). Pursuant to 18 U.S.C. § 2703, I seek a warrant requiring Apple Inc. to disclose records and information in connection with a criminal investigation. This Court has authority under 18 U.S.C. § 2705(b) to issue "an order commanding a provider of electronic communications service or remote computing service to whom a warrant . . . is directed, for such period as the court deems appropriate, not to notify any other person of the existence of the warrant. . ." Id.

37. Here, such an order is appropriate because the requested warrant relates to an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation, and its disclosure may alert the targets to the ongoing investigation. Accordingly, there is reason to believe that notification of the existence of the requested warrant will seriously jeopardize the investigation, by giving targets an opportunity to destroy or tamper with evidence or otherwise seriously jeopardize an investigation. See 18 U.S.C. § 2705(b).

CONCLUSION

38. Based on the forgoing, I request that the Court issue the proposed search warrant. Because the warrant will be served on Apple who will then compile the requested records at a time convenient to it, there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night.

39. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that – has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

40. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

Dated this 10th day of July 2020.

WILLIAM FULTON
Special Agent, ATF

Subscribed and sworn to before me telephonically on 10th day of July 2020.

PETER OPPENEER
United States Magistrate Judge

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with sire.gq@icloud.com that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at 1 Infinite Loop, Cuptertino, CA 95014.

ATTACHMENT B[3]

Particular Things to be Seized

I. Information to be disclosed by Apple

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, including any messages, records, files, logs, or information that have been deleted but are still available to Apple, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government, in unencrypted form whenever available, for each account or identifier listed in Attachment A:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, methods of connecting, and means and source of payment (including any credit or bank account numbers);

---

[3] The United States, and its forensic and law enforcement partners (the government), will seize the information described herein only for investigative purposes and for probable discovery pursuant to *Brady v. Maryland,* 373 U.S. 83 (1963), *Giglio v. United States*, 405 U.S. 150 (1972), and Federal Rules of Criminal Procedure 16(a)(1)(E) and 26.2. The government will examine the seized information to identify information that is relevant to the matter under investigation and will thereby exercise respect for the information owner's personal and Constitutional privacy interests. Litigants are invited to contact the assigned AUSA to address privacy or other concerns.

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers ("GUID"), Media Access Control ("MAC") addresses, Integrated Circuit Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers ("MSISDN"), International Mobile Subscriber Identities ("IMSI"), and International Mobile Station Equipment Identities ("IMEI");

c. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. The contents of all instant messages associated with the account, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and

length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWorks (including Pages, Numbers, and Keynote), iCloud Tabs, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), messaging logs (including iMessage, SMS, and MMS messages), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find my iPhone logs, logs associated with iOS device activation and upgrades, and logs associated with web-based access of Apple services (including all associated identifiers);

g. All records and information regarding locations where the account was accessed, including all data stored in connection with Location Services;

h. All records pertaining to the types of service used; and

i. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken.

II. **Information to be seized by the government**

a. All information described above that constitutes evidence of violations of 18 U.S.C. § 844(i), as well as contraband, and property designed for use, intended for use, or used in committing those crimes involving Marquon Clark since June 10, 2020, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

b. The identity of the person who created or used the Apple ID, including records that help reveal the whereabouts of such person;

c. Evidence indicating how and when the account was accessed or used, to determine the chronological and geographic context of account access, use and events relating to the crime under investigation and the account subscriber;

d. Evidence indicating the subscriber's state of mind as it relates to the crime under investigation;

e. Photographs of medical information and communication related to those photographs; and

f. Evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts.